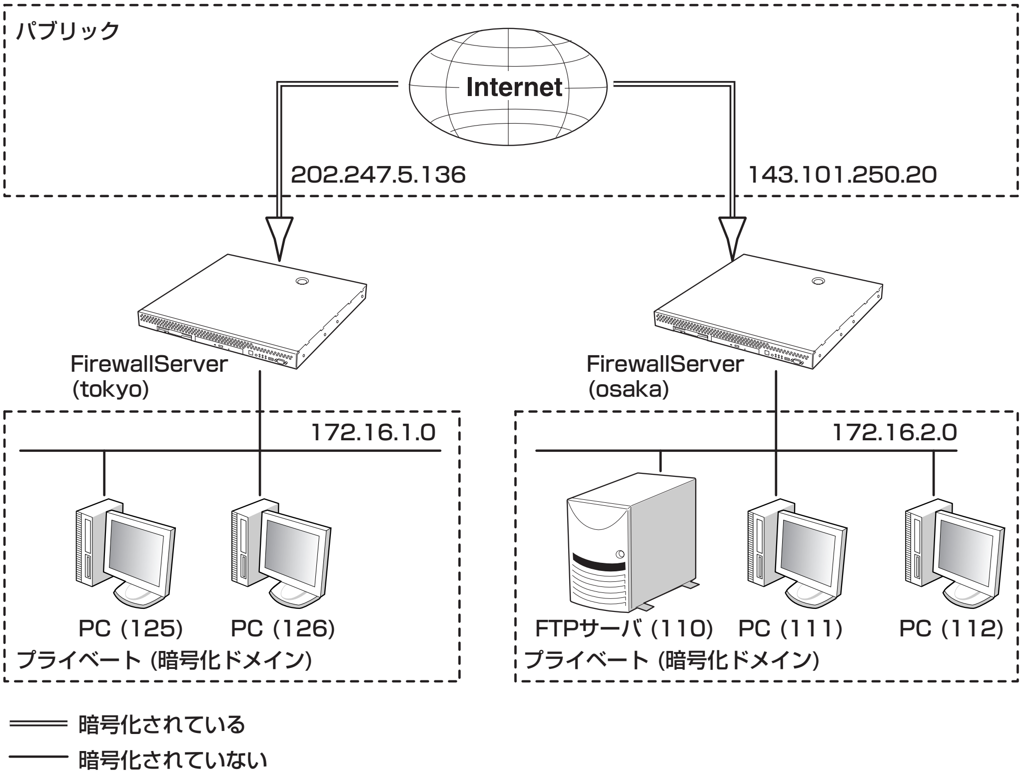
3 Virtual Private Network(VPN)

本章では、FirewallServerを使用してVPN(Virtual Private Network)環境を構築するための手順を説明します。ここで示しているのは一例です。実環境ではネットワーク構成・セキュリティポリシー等により作成手順は異なります。

FireWall-1、VPNの設定方法およびPolicy Editorの使用方法の詳細に関してはCheck Point Next Generationに付属のマニュアルを参照してください。

エクストラネットVPNの設定

この章では下図のネットワーク環境のように、2台のFirewallServer間（tokyo－osaka）でVPN環境を構築する際の手順を説明します。
暗号化方式はIKEを使用した例です。その他の暗号化方式を使用する場合や詳細な設定方法に関してはCheck Point Next Generationに付属のマニュアルを参照してください。



設定手順の流れ

VPN構築手順は、下図に従って説明します。

前準備 →86ページ

1. GUIクライアントのセットアップ

↓

2. 前提条件の設定

⇩

セットアップ（東京側／大阪側） →87ページ〜94ページ

1. オブジェクトの作成
   - （1）ゲートウェイのワークステーション・オブジェクトの作成
   - （2）ネットワーク・オブジェクトの作成

↓

2. 鍵ネゴシエーションの設定
   - （1）暗号化ドメイン作成とネットワーク・オブジェクトの登録
   - （2）暗号化ドメインの登録
   - （3）認証方式の設定

↓

3. 暗号化の設定
   - （1）セキュリティーポリシーの作成
   - （2）暗号化の設定
   - （3）セキュリティーポリシーのインストール

前準備

GUIクライアントのセットアップ

GUIクライアントのセットアップについては2章を参照してください。

前提条件の説明

東京と大阪にある2つのローカルネットワーク間で、VPNを利用したftpサービスを実現する方法を説明します。
以降の手順では、東京側のクライアントから大阪側のftpサーバに接続することができるように、オブジェクトを設定し、セキュリティポリシーにルールを追加します。ここでは、以下の条件でローカルネットワークが構成されていることを前提に話を進めます。

	東京側の設定	大阪側の設定
firewallのオブジェクト名	tokyo	osaka
IPアドレス	eth0(外側) 202.247.5.136 eth1(内側) 172.16.1.0	eth0(外側) 143.101.250.20 eth1(内側) 172.16.2.20
ローカルネットワーク	ネットワークアドレス 172.16.1.0 ネットマスク 255.255.255.0	ネットワークアドレス 172.16.2.0 ネットマスク 255.255.255.0

セットアップ

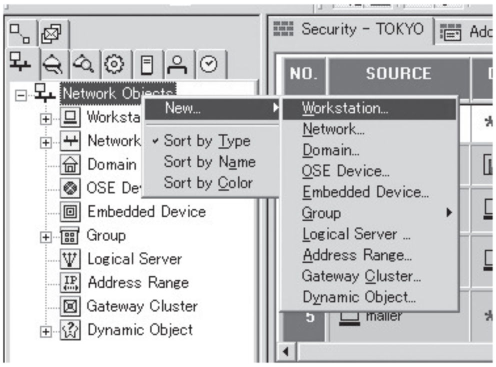
まず最初にFirewallServer tokyoとosakaでお互いの鍵をネゴシエーションする方式とデータを暗号化する方式を設定しておく必要があります。
以下の設定手順の流れに従って、東京側の設定手順を説明します。大阪側の設定に関しては、注意書きを参考にして同様に設定してください。

オブジェクトの作成

ワークステーションオブジェクトおよびネットワークオブジェクトを作成します。

ゲートウェイのワークステーション・オブジェクトの作成

ここでは、鍵ネゴシエーションや暗号化に必要なオブジェクトを作成する方法を説明します。Policy Editorを起動し、接続されたらオブジェクトツリーパネル内の[Network Objects]を右クリックし[New]-[Workstation]を選択します。



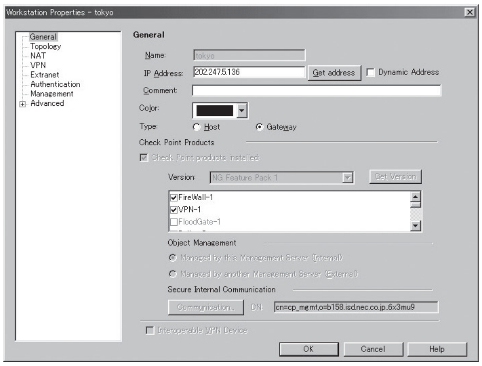
設定は、以下の手順で行います。

1. Name、IP Addressにマシン名、IPアドレスを入力する。
2. 「Check Point products installed」にチェックを入れ、「FireWall-1」と「VPN-1」を選択する。
3. Object Managementの項目は、デフォルト設定のままでManaged by this Management Server (Internal)とする。

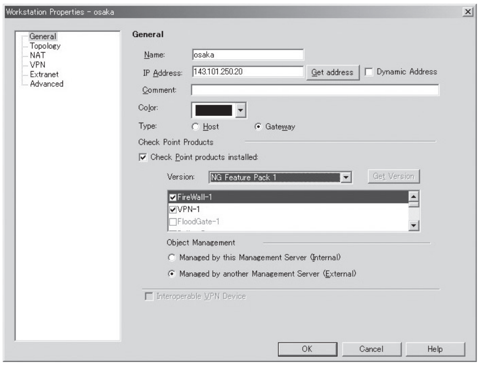
osakaの設定*も上記と同様に行います。ただし、Object Managementの項目は、「Managed by another Management Server(External)」を選択します。

* 大阪側の設定においてはosakaをInternal、tokyoをExternalと設定します

<ワークステーションゲートウェイの作成>



tokyoのWorkstation Propeties

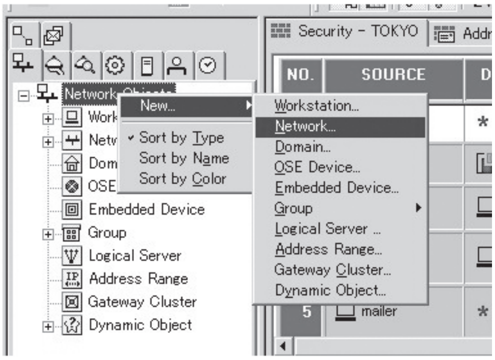


osakaのWorkstation Propeties

ネットワーク・オブジェクトの作成

次に、保護すべきtokyo側のローカルネットワークとosaka側のローカルネットワークのネットワーク・オブジェクトを作成します。(ここでは、tokyo_local_networkという名前でネットワーク・オブジェクトを作成して、説明します)

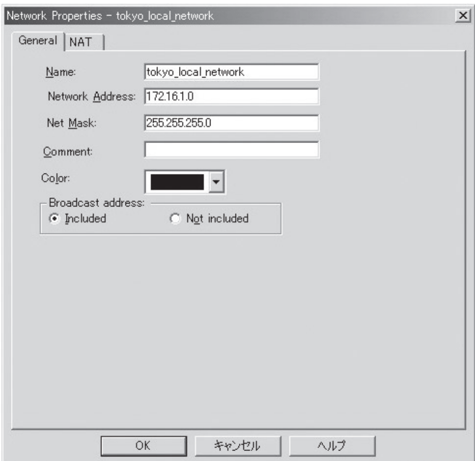
また、同様にosakaのプライベートネットワークのネットワーク・オブジェクトも作成します。
まず、オブジェクトツリーパネル内の[Network Objects]を右クリックし[New]-[Network]を選択します。
設定は以下の手順で行います。



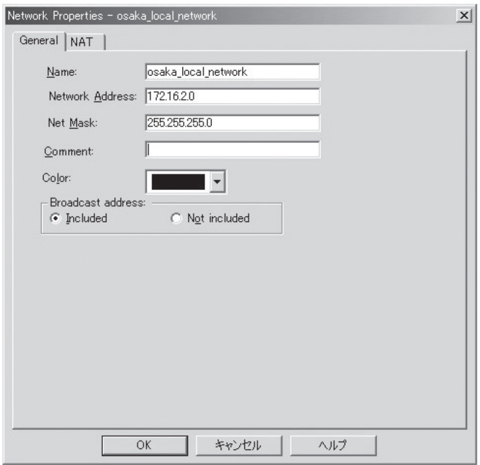
1. Nameにネットワーク・オブジェクト名を入力する。

2. Network Address、Net Maskをそれぞれ入力する。

同様に大阪側の設定も行ってください。



tokyoのプライベートネットワーク



osakaのプライベートネットワーク

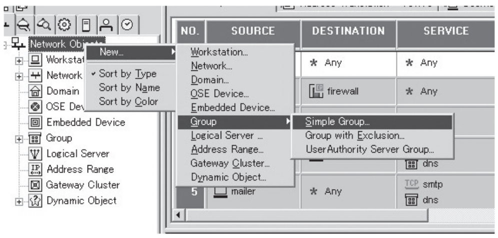
鍵ネゴシエーションの設定

鍵ネゴシエーションを設定します。

暗号化ドメインの作成とネットワーク・オブジェクトの登録

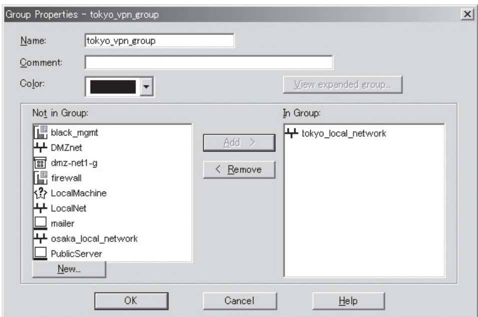
ここでは暗号化対象のネットワークあるいはホストを登録する暗号化ドメイン(グループ)の作成手順について説明します。

まず、オブジェクトツリーパネル内の[Network Objects]を右クリックし[NEW]-[Group]-[SimpleGroup]を選択しtokyo側の暗号化ドメインを作成します。

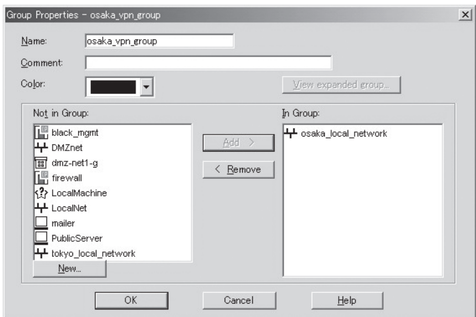


作成した暗号化ドメインに前述で作成したネットワーク・オブジェクト「tokyo_local_network」を選択しIn Groupへ移動させてください。(ここでは、暗号化ドメインをtokyo_vpn_groupとして作成します)

同様にosaka側の暗号化ドメインも作成してください。



tokyoの暗号化ドメイン

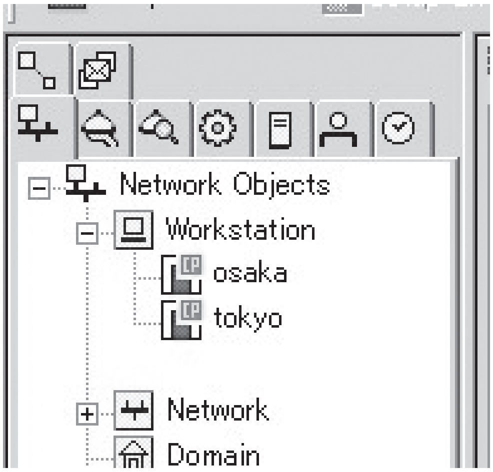


osakaの暗号化ドメイン

暗号化ドメインの登録

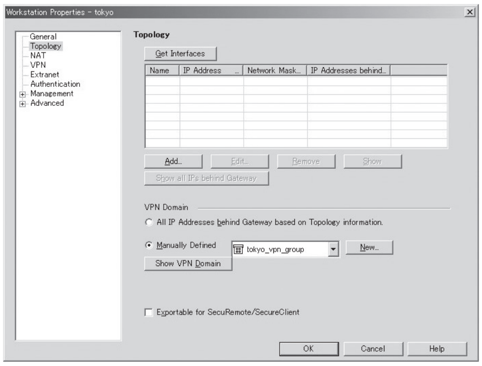
ここでは、作成した暗号化ドメインを前述で作成したゲートウェイに登録する方法を説明します。この登録により、FirewallServerに暗号化対象のネットワークおよびホストを認識させせます。

まず、前述で作成したｔｏｋｙｏのWorkstation Propertiesウィンドウを開きます。

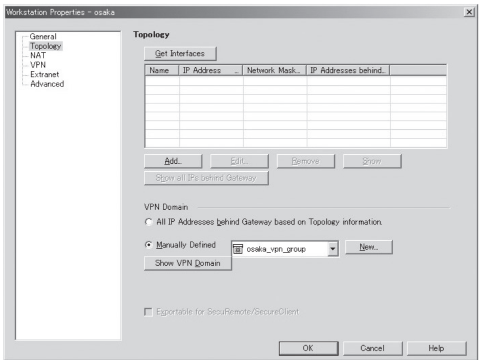


次にTopologyページを開きVPN Domainの項目にて「Manually Defined」を選択し、前述で作成した暗号化ドメイン「tokyo_vpn_group」を選択します。
osaka側も同様に暗号化ドメイン「osaka_vpn_group」を選択します。

＜各ゲートウェイへの暗号化ドメインの登録＞



tokyoの暗号化ドメインの登録



osakaの暗号化ドメインの登録

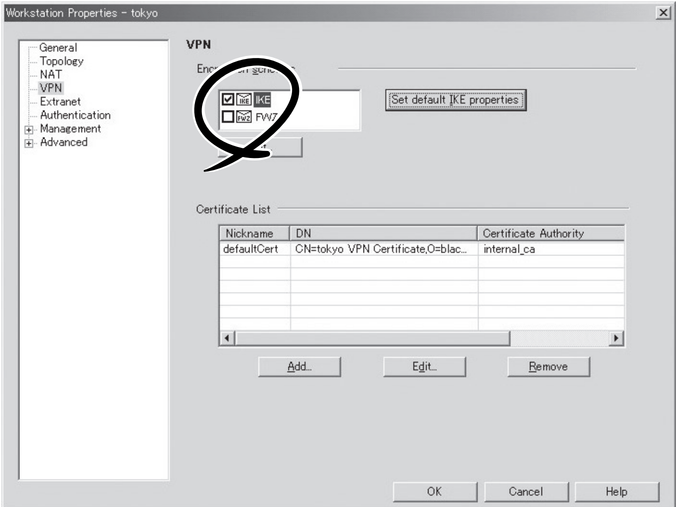
認証方式の設定

東京と大阪で行う認証方式の設定を説明します。(ここでは、IKEの場合を説明します)

まず先ほどのWorkstation Propertiesウィンドウから、VPNページを開きます。

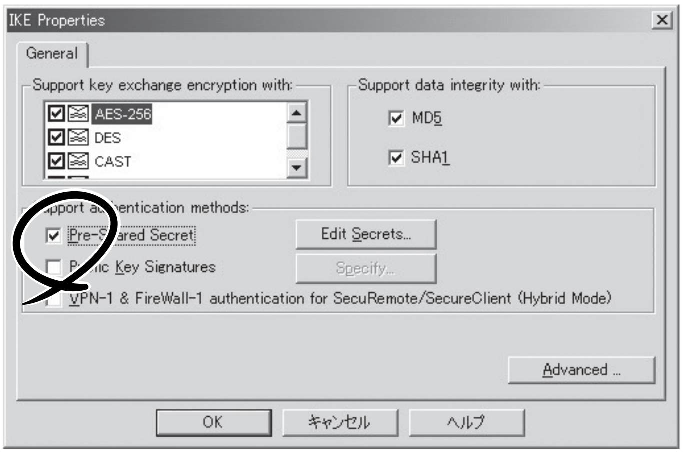
設定は、以下の手順で行います。

1. Encryption schemesの｢IKE｣をチェックする。



2. [Edit...]をクリックし、IKE Propertiesウィンドウを開く。

3. Support authentication methodsの、[Pre-Shared Secret]にチェックをする。



4. [OK]をクリックし、IKE Propertiesウィンドウを閉じる。

続けてosakaもtokyoと同様に設定します。
ただし、osakaでは以下の設定が必要となります。

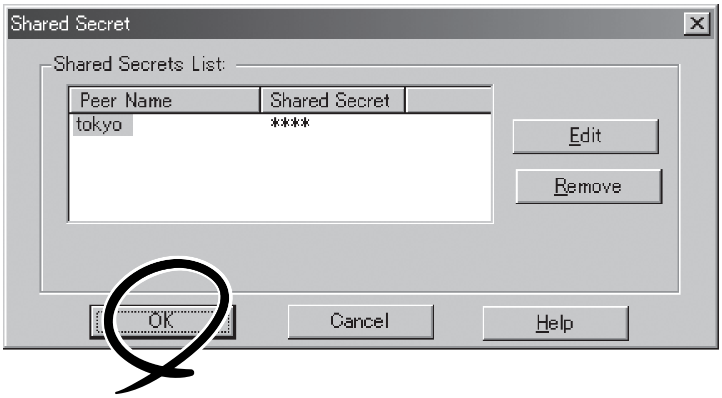
1. [Edit Secrets]をクリックして、Shared Secretウィンドウを開く。

2. Shared Secrets Listにtokyoのワークステーションが表示されているので、「tokyo」ワークステーションを選択し、[Edit]をクリックする。

3. 次にShared Secretを入力するテキスト・ボックスが表示されるので、下記の条件にしたがって入力する。

   ・6文字以上16文字以下で入力してください。
   ・FireWall-1/VPN-1で使用する予約語は使用できません。

4. [Set]をクリックして、[OK]をクリックし、Shared Secretウィンドウを終了させる。



以上で鍵ネゴシエーションの設定は終了です。
同様に大阪側の設定も行ってください。(tokyoとosakaを置き換えて設定)

暗号化の設定

暗号化ルールの設定をします。

セキュリティポリシーの作成

東京側のネットワークから、大阪側のネットワークへの通信を暗号化するために、以下の設定内容を参考にルールを追加します。
同様に大阪側の設定も行ってください。

設定事項

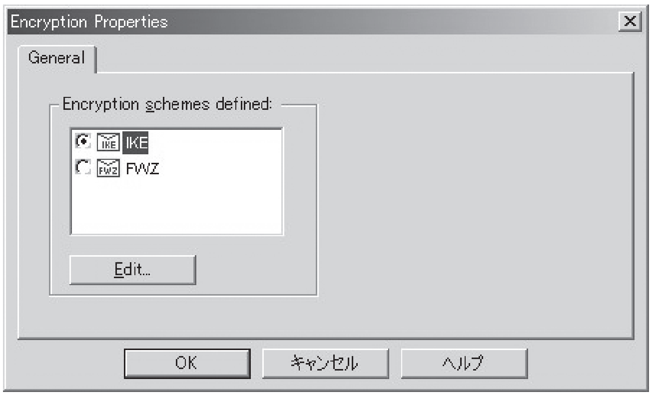
Source	tokyo_local_network
Destination	osaka_local_network
Service	ftp
Action	Encrypt



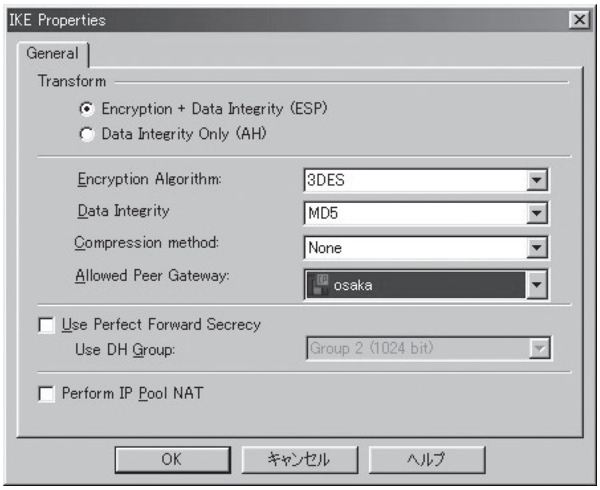
暗号化の設定

1. ルールのActionカラムの「Encrypt」を選択して、Encryption Propertiesウィンドウを開く。

2. Encryption Propertiesウィンドウの[General]タブから「IKE」を選択して[Edit…]をクリックし、IKE Propertiesウィンドウを開く。（このウィンドウでは、ルールが適用される接続を暗号化するのに使用するIPSec方式を定義します。）



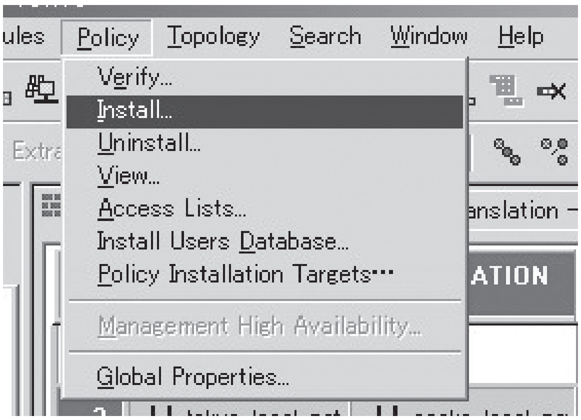
3. Allowed Peer Gatewayにおいて通信先のFirewallServerである「osaka」ワークステーションを選択する。



通常は、Allowed Peer Gatewayのプルダウンタブ以外は、デフォルトのままで問題ありません。

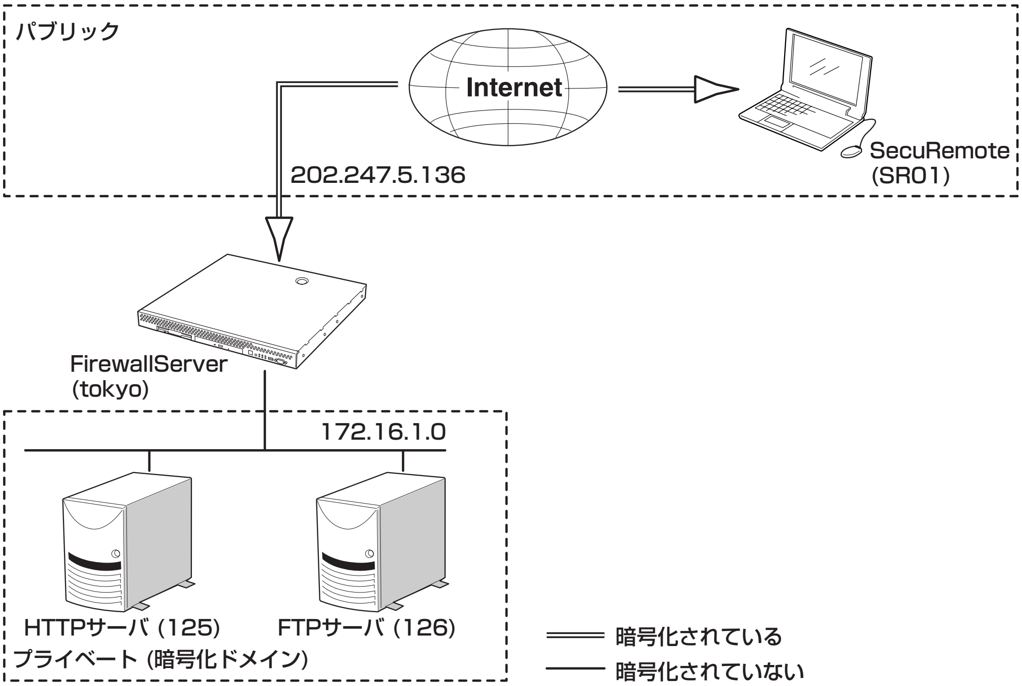
セキュリティポリシーのインストール

最後に、作成したルールを有効にする必要があります。Policy Editorのメニューバーから[Policy]-[Install]を選択しセキュリティポリシーのインストールを行い、作成したルールを有効にしてください。



リモートアクセスVPNの設定

SecuRemoteを使用することで、モバイルおよびリモートユーザーがインターネットに接続された企業ネットワークへ安全にアクセスすることが可能になります。ここでは、下図のようにSecuRemoteとFirewallServer間(SR01-tokyo)で、VPN環境を構築する際の手順を説明します。暗号化方式はIKEを使用した例です。その他の暗号化方式を使用する場合や詳細な設定方法に関しては、Check Point Next Generationに付属のマニュアルを参照してください。



設定手順の流れ

リモートアクセスVPN構築手順は、以下の図に従って説明します。

前準備
→97ページ～98ページ

1. GUIクライアントのセットアップ
2. 前提条件の説明
3. SecuRemoteのダウンロード

FirewallServerの設定
→99ページ～106ページ

1. 暗号化方式の設定
   - (1) 暗号化ドメインの設定
   - (2) 認証方式の選択
2. ユーザーの定義
   - (1) ユーザーの作成
   - (2) ユーザの暗号化方式の設定
   - (3) ユーザの認証方式の設定
   - (4) ユーザグループの作成とユーザの登録
3. グローバルプロパティの設定
4. ポリシーの設定
   - (1) セキュリティポリシーの作成
   - (2) セキュリティポリシーのインストール

SecuRemoteのインストール
→107ページ～108ページ

SecuRemoteの設定
→109ページ～110ページ

1. サイトの設定
2. サイト情報のダウンロード

SecuRemoteの使用方法
→111ページ

前準備

次の順序に従ってセットアップの前準備をします。

GUIクライアントのセットアップ

GUIクライアントのセットアップについては2章を参照してください。

前提条件の説明

SecuRemoteと東京にあるローカルネットワークの間で、VPNを利用したftpサービスを使用できるようにします。
以降の手順では、SecuRemoteから東京側のftpサーバに接続することができるように、オブジェクトを設定しセキュリティポリシーにルールを追加します。
ここでは以下の条件でローカルネットワークが構成されていることを前提に説明を進めます。

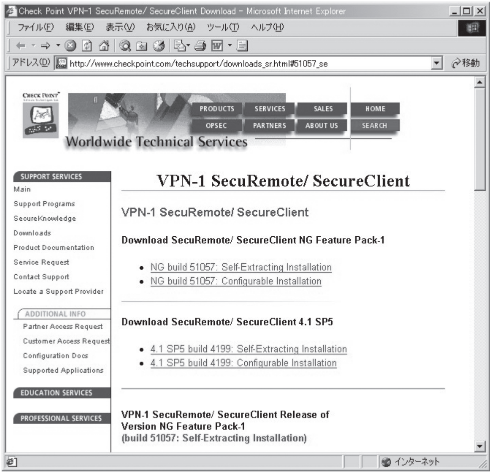
設定内容

firewallのオブジェクト名	tokyo
IPアドレス	eth0(外側)： 202.247.5.136 eth1(内側)： 172.16.1.0
ローカルネットワーク	ネットワークアドレス：172.16.1.0 ネットマスク： 255.255.255.0

SecuRemoteのダウンロード

リモートユーザーが暗号化通信を行うにはクライアントPCにSecuRemoteが必要です。SecuRemoteはCheck Point Next GenerationのCD-ROMにも収録されていますが、最新版をwebからダウンロードして使用されることをお勧めします。
最新版のSecuRemoteは下記URLからダウンロードしてください。

http://www.checkpoint.com/techsupport/freedownloads.html



このページでは、以下の二種類のダウンロードが可能となっています。

- Download SecuRemote/SecureClient NG Feature Pack-1
- Download SecuRemote/SecureClient 4.1 SP5

Download SecuRemote/SecureClient NG Feature Pack-1の方から、自己解凍型ファイルまたは、tgzファイルのどちらか一方を選択し、ダウンロードしてください。
ただし、以降の手順では、自己解凍形式(Self-Extracting Installation)を選択したものとして手順を記します。
SecuRemote対応プラットフォームは以下のとおりです。

- Windows 98
- Windows Me
- Windows NT 4.0
- Windows 2000
- Windows XP

上記は2002年3月現在の情報です。最新の対応状況等についてはRelease Notesで確認してください。

FirewallServerの設定

SecuRemoteを使用するためには、FirewallServer(tokyo)側で以下の項目を設定しておく必要があります。

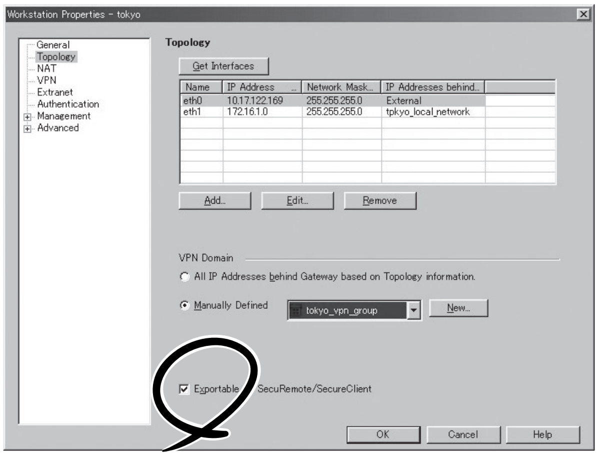
- 暗号化通信で使用する鍵のネゴシエーション方式の設定
- データを暗号化する方式の設定
- ユーザーの設定

暗号化方式の設定

暗号化通信に使用する鍵をネゴシエーションする方式と、データを暗号化する方式を設定します。この内容に関しては、「エクストラネットVPNの設定」を参照してください。
ただし、以下の点に注意してください。

暗号化ドメインの登録の時

SecuRemoteからの接続を許可するために、「Exportable for SecuRemote/ SecuClient」にチェックします。

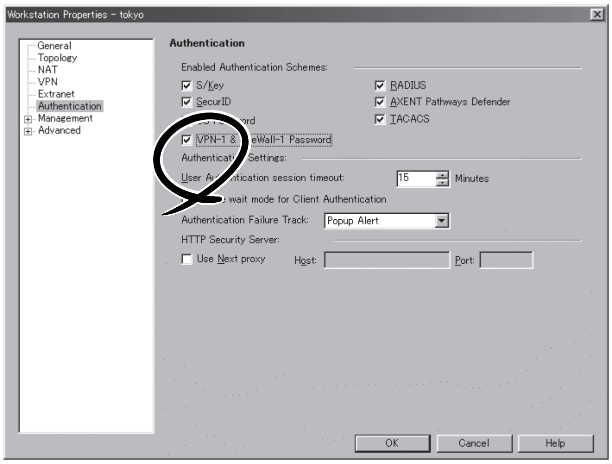


認証方式の選択の時

Support authentication methods:で「VPN-1&FireWall-1 authentication for SecuRemote/SecuClient (Hybrid Mode)」にチェックします。



次に、tokyoのWorkstation Properties-Authenticationページを開きます。
その中の、「Enabled Authentication SchemesのVPN-1&FireWall-1 Password」にチェックして[OK]をクリックし、Workstaion Propertiesウィンドウを閉じます。



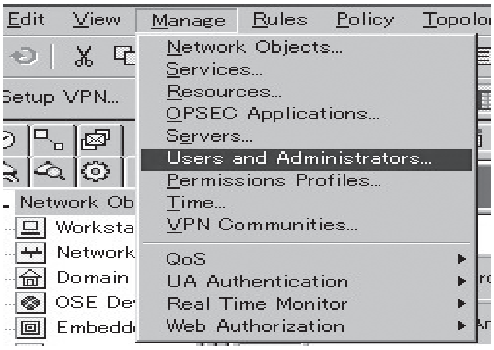
ユーザーの定義

ユーザーの設定をします。

ユーザーの作成

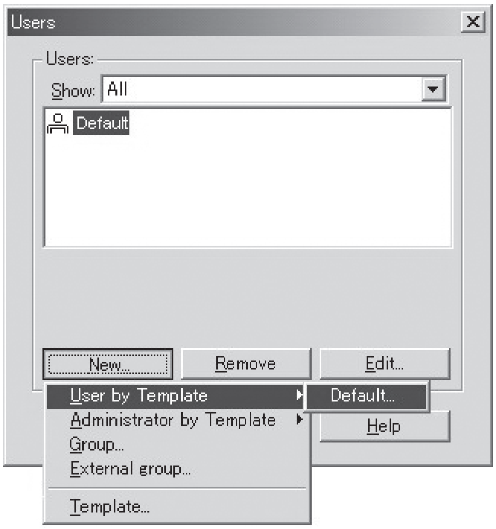
設定は、以下の手順で行います。

1. Policy Editorでメニューバーの[Manage]-[Management Users and Administrators]を選択しUsersウィンドウを開く。



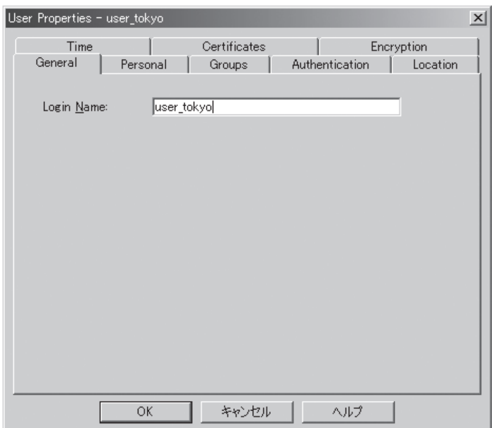
2. SecuRemoteを使用するユーザーを登録する。

   [New]をクリックした後、[User by Template]-[Defalt]を選択し、User propertiesウィンドウを開きます。



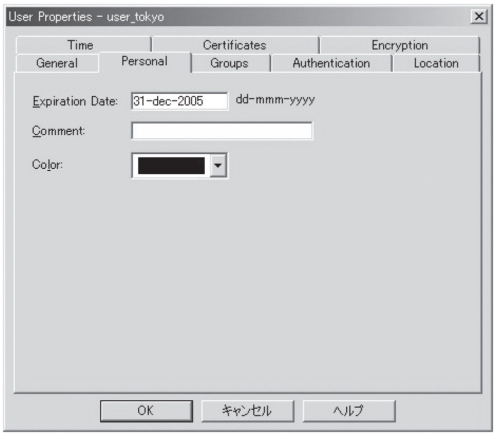
3. [General]タブを開く。

   NameにSecuRemoteを使用するユーザー名(user_tokyo)を入力する。



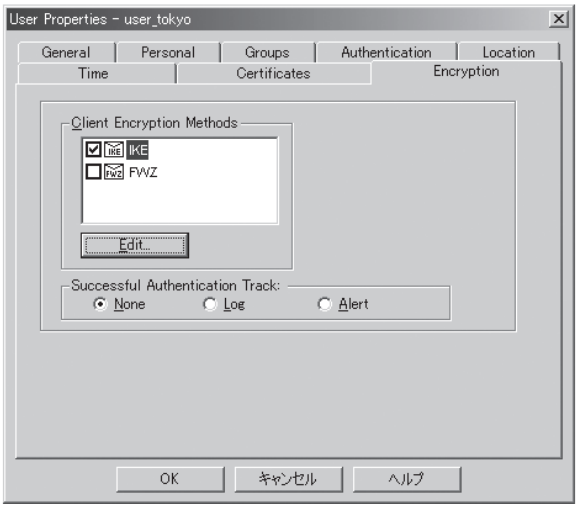
4. [Personal]タブを開く。

Expiration Dateには、このユーザーの有効期限を設定します。デフォルトでは、31-dec-2002となっていますので、必ず正しい有効期限を設定してください。



ユーザーの暗号化方式の設定

[Encryption]タブを開きます。
Client Encryption Methodsの中にある「IKE」をチェックして、暗号化方式をIKEに設定します。

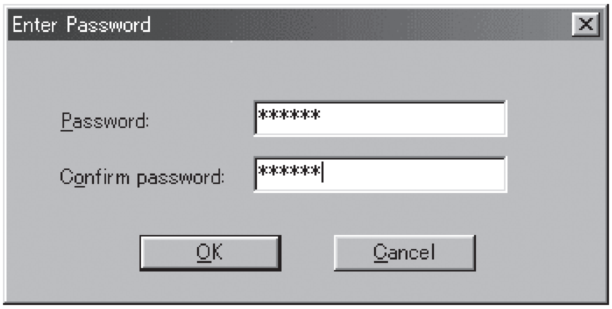


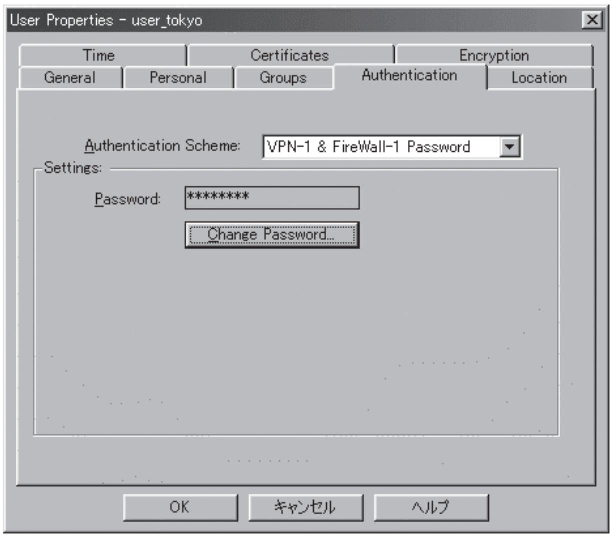
ユーザーの認証方式の設定

1. [Authentication]タブを開く。

   Authentication Schemeで「VPN-1&FireWall-1 Password」を選択し、[Change Password]をクリックして表示されたEnter Passwordウィンドウで以下の条件に従ってパスワードを設定します。

   ・ 4 文字以上 8 文字以下で入力してください。
   ・FireWall-1/VPN-1で使用する予約語は 使用できません。





2. 設定が終わったら[OK]をクリックしてUsers Protatiesウィンドウを閉じる。

ユーザーグループの作成とユーザーの登録

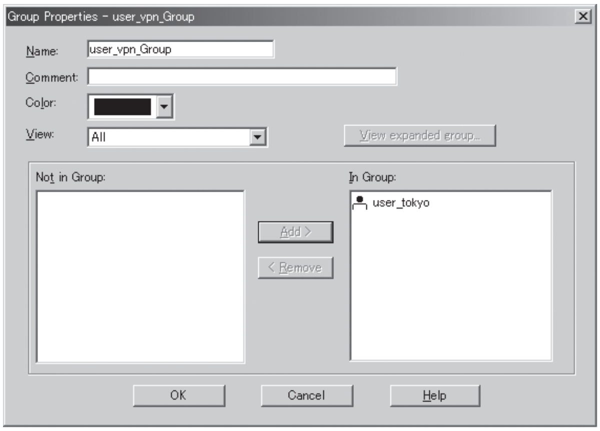
1. Usersウィンドウの[NEW]をクリックし、「Group」を選択してGroup Propertiesウィンドウを開く。

2. NameにSecuRemoteを使用するユーザーグループ名(user_vpn_Group)を入力する。

3. 前項で作成したユーザー(user_tokyo)がNot in Groupに表示されているので、これを選択し[Add]をクリックする。

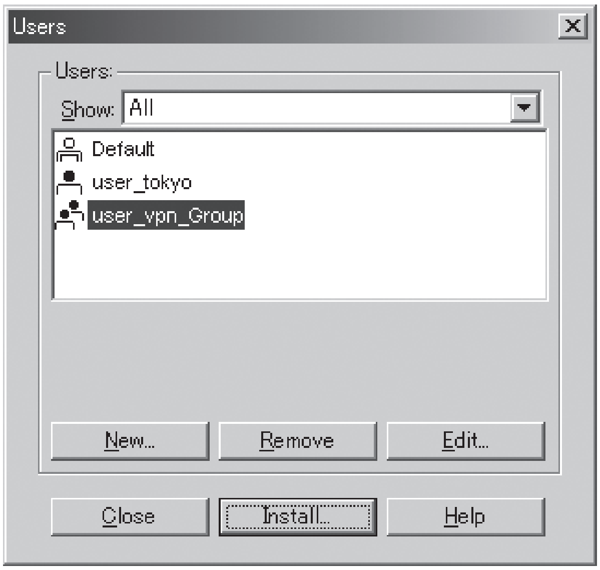
4. 選択したユーザーがIn Groupへ移動したことを確認して[OK]をクリックする。

   Group Propertiesウィンドウを閉じます。



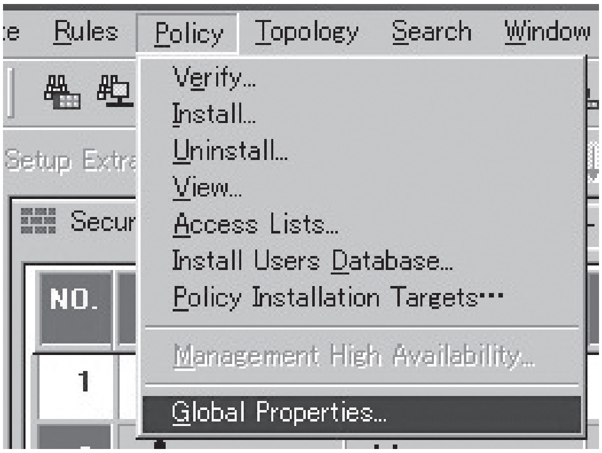
5. Usersウィンドウで、[Install]をクリックする。

   作成したユーザーおよびユーザーグループを有効にします。

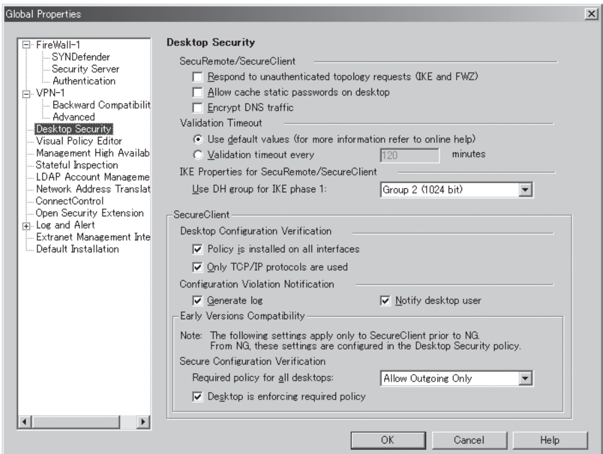


グローバルプロパティの設定

1. Policy Editorでメニューバーから[Policy]-[GobalProperties]を選択する。



2. Desktop Securityページを開き、SecuRemote/SecureClientで「Respond to unauthenticated topology requests(IKE and FWZ)」のチェックをはずす。



✔ チェック

このオプションがチェックされている場合、SecuRemoteがサイト情報のダウンロードに失敗することがあります。

ポリシーの設定

暗号化ルールの設定をします。

セキュリティポリシーの作成

SecuRemoteから、東京側のネットワークへの通信を暗号化するために以下の設定内容でルールを追加します。

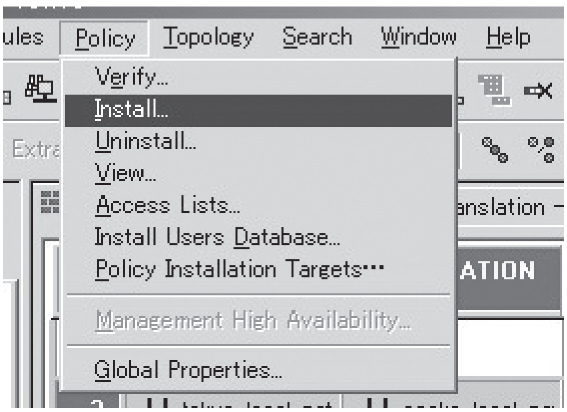
設定内容

Source	user_vpn_Group
Destination	tokyo_local_network
Service	ftp
Action	Client Encrypt



セキュリティポリシーのインストール

最後に、作成したルールを有効にする必要があります。Policy Editorのメニューバーから[Policy]-[Install]を選択しセキュリティポリシーのインストールを行い、作成したルールを有効にしてください。



SecuRemoteのインストール

クライアントPCにSecuRemoteをインストールする手順について説明します。

1. 前準備でダウンロードした自己解凍形式ファイルを、ダブルクリックしてインストールを始める。

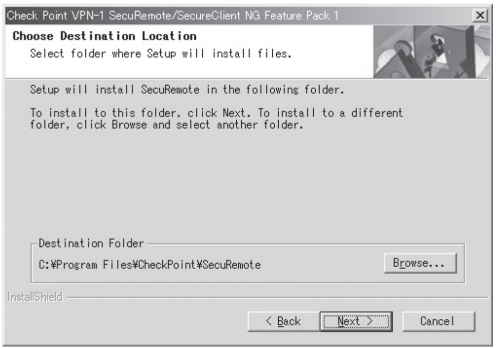
2. Welcome画面が表示されるので、[Next]をクリックする。

3. 使用許諾契約書が表示されるので、内容をよく読み、同意する場合は[Yes]をクリックする。同意しない場合は[No]をクリックして終了する。

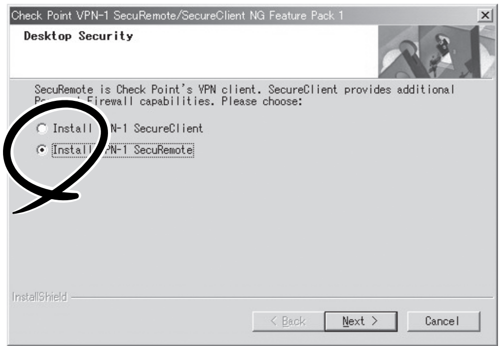
4. インストール先のフォルダを指定する画面が表示されるので、必要に応じてフォルダを変更する。

5. インストール先のフォルダを確認したら[Next]をクリックする。

   ファイルのコピーが開始されます。

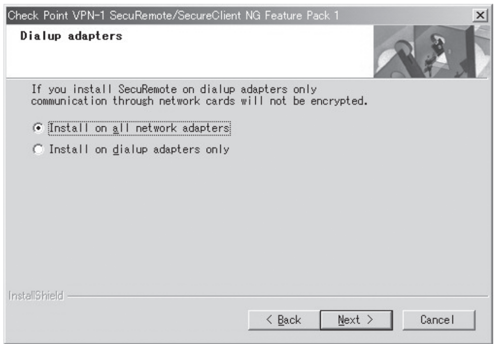


6. 選択画面が表示されるので、「Install VPN-1 SecuRemote」をチェックし、[Next]をクリックする。



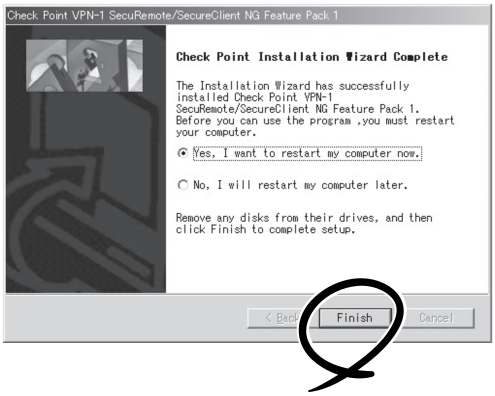
7. どのアダプタにSecuRemoteをインストールするかを指定する。

   どちらを選択するかはシステム管理者に確認してください。



8. 右図のメッセージが表示されたら、[Finish]をクリックして再起動する。

再起動後に、新しい構成が有効になります。



SecuRemoteの設定

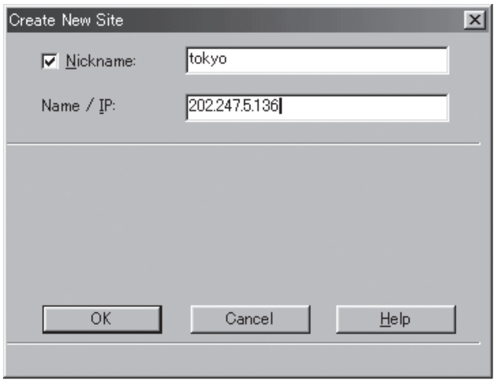
インストールしたSecuRemoteの設定をします。

サイトの設定

SecuRemoteを使用して通信する前に、通信相手のサイト(tokyo)を定義する必要があります。（サイトの定義をするには、SecuRemoteがインストールされているPCがネットワークに接続されている必要があります。）

設定は、以下の手順で行います。

1. Sitesメニューを開き、[New Sites]-[Create New]を選択する。
2. Create New SiteウィンドウのNicknameにサイト名(tokyo)を入力し、Name/IPに解決可能なホスト名またはIPアドレスを入力する。
3. サイトの情報を入力したら、[OK]をクリックする。



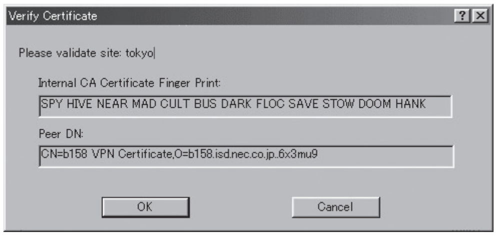
サイト情報のダウンロード

1. サイトの設定に間違いがなく、サイト側(tokyo)の設定が適切にされると、VPN-1 SecuRemote Authenticationウィンドウが表示される。



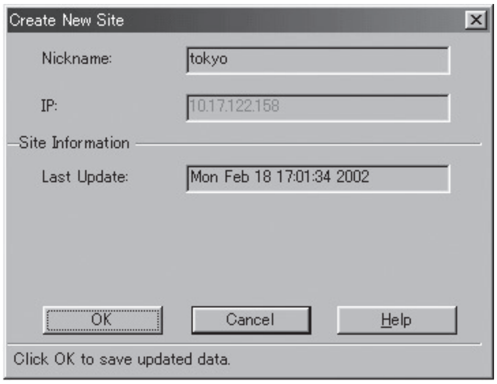
2. User nameとPasswordを入力し[OK]をクリックする。

   Verify Certificateウィンドウが表示されます。



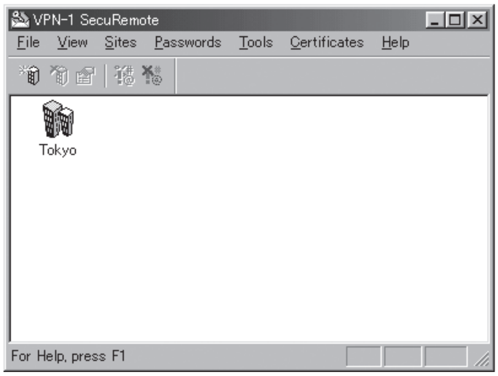
3. [OK]をクリックする。

   サイト情報がダウンロードされ、Create New Siteウィンドウが表示されます。



4. [OK]をクリックする。

   定義したサイト(tokyo)のアイコンがメインウィンドウ内に作成されます。



以上でSecuRemote(SR01)側の設定は終了です。

SecuRemoteの使用方法

SecuRemoteを使用して暗号化通信を行うにあたり、SecuRemoteクライアントが最初にサイトへの接続する場合に認証が行われ、下図のようにユーザー名とパスワードを入力するウィンドウが表示されます。
ユーザーは自ユーザー名とパスワードを入力します。認証に成功すると以降の接続時にはウィンドウは表示されません。



~Memo~